

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

3/9/2010

SUBJECT:

Vulnerability in Windows Movie Maker and Microsoft Producer Could Allow Remote Code Execution (MS10-016)

OVERVIEW:

A vulnerability has been discovered in Windows Movie Maker and Microsoft Producer which could allow an attacker to take complete control of an affected system. Windows Movie Maker is a video editing application available for Microsoft Windows, which is installed by default on Windows XP systems. Microsoft Producer is a downloadable add-in component for Microsoft Office PowerPoint that can be used open and edit video files. Exploitation may occur if a user visits a web page or opens an email attachment which is crafted specifically to take advantage of this vulnerability. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. At this point in time, no patches are available for Microsoft Producer.

SYSTEMS AFFECTED:

Windows XP
Windows Vista
Windows 7
Producer 2003

RISK:

Government:

Large and medium government entities: High
Small government entities: High

Businesses:

Large and medium business entities: High
Small business entities: High

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Windows Movie Maker and Microsoft

Producer which could allow an attacker to take complete control of an affected system. This is due to the way that Windows Movie Maker and Microsoft Producer parse specially crafted Movie Maker Project files (.mswmm) or Microsoft Producer 2003 files (.MSProducer, .MSProducerZ, and .MSProducerBF). This vulnerability can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Windows Movie Maker or Microsoft Producer project file as an email attachment. In the Web based scenario, a user would have to open a specially crafted Movie Maker or Microsoft Producer file that is hosted on a website.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

At this point in time, no patches are available for Microsoft Producer.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider blocking .MSWMM files at the network perimeter.
- Consider removing the Movie Maker .MSWMM file association.
- Consider removing the Microsoft Producer 2003 (.MSProducer, .MSProducerZ, and .MSProducerBF) file association (<http://support.microsoft.com/kb/975561>).
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open email attachments from unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS10-016.mspx>

<http://support.microsoft.com/kb/975561>

Security Focus:

<http://www.securityfocus.com/bid/38515>